UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,385	12/06/1999	OLEG ANATOLIVICH ZOLOTOREV	P-9901MG	9875

7590 08/27/2003

LACKENBACH SIEGEL MARZULLO
ARONSON & GREENSPAN
ONE CHASE ROAD
PENTHOUSE SUITE
SCARSDALE, NY 10583

EXAMINER
HO, THOMAS M

ART UNIT	PAPER NUMBER
2134	3

DATE MAILED: 08/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/445,385	ZOLOTOREV ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☒ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-29* is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12/06/99* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-29 are pending.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed in record of file. However, the applicant discloses in the Foreign PCT/RU98/00197, a UHF filter comprising a dual-mode resonator formed on a wave-guide having a round cross-section. The disclosed priority data appears to have no relevance to the applicant's application for a "Method for making a Blind RSA-Signature and apparatus therefor". In consequence, the applicant's claim for the priority claim has not been granted at this time. It appears that it was the intention of the applicant to disclose PCT/RU99/00197, "Method for the Blind Generation of a Digital RSA Signature and Device for Realising the Same" as the priority data.

Drawings

3. The drawings are objected to under 37 CFR 1.83(a) because they fail to show textual labels as described or mentioned in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). For example, on page 17 of the specification, the applicant additionally refers to element 6 of figure 2 as an "arithmetic controller", and element 7 as an "inadmissible divisor input". The drawings should be amended with the applicant's textual references accompanying their

respective numbers within the drawings to allow for a proper understanding of the disclosed invention. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawing will not be held in abeyance.

Allowable Subject Matter

4. The following is the examiner's statement for reasons of allowance:

In reference to claim 1:

Applicant properly identifies that Chaum, U.S. Patent No. 4,759,064 is relevant prior art on page 3 of the application. Chaum discloses a Blind Signature System comprising the steps of: "choosing secret factors (Chaum column 1, lines 22-24) and an RSA module corresponding to them(Chaum column 1, lines 27), choosing at least one admissible public RSA-exponent(Chaum column 1, lines 24-25), choosing initial data (Chaum column 1, lines 28), choosing a randomized blinding key(Chaum column 1, lines 44-45), choosing an encryption RSA-key whose module corresponds to the chosen RSA-module and whose exponent corresponds to the chosen blinding key with which key an RSA-encryption is performed while creating blinded data(Chaum column 1, lines 25-27, lines 44-47), arbitrarily choosing a secret RSA-key corresponding to the chosen secret factors and an arbitrary admissible public RSA-exponent (Chaum column 1, lines 26-30 and lines 43-45) and creating a digital RSA-signature on the blinded data corresponding to said secret RSA-key(Chaum column 1, lines 44-47), unblinding the created digital RSA-

signature on the blinded data by inputting the digital RSA-signature on the blinded data, the blinding key, the RSA module, and the public RSA-exponent corresponding to the secret RSA-key used in creating the digital RSA-signature on the blinded data, into an unblinding converter whose output data are obtained as the digital RSA-signature on the chosen initial data." (Chaum column 1,lines 43-47)

Chaum, and the remaining art of record however, fails to disclose a system where a masking factor coprime to each admissible public RSA-exponent is additionally chosen and where the blinding key is chosen coprime to each admissible public RSA-exponent as a multiple to the chosen masking factor. From the context of page 4 of the specification, it is understood that "multiple" refers only to integer multiples. Within the specification, the applicant reveals the randomized blinding key R to be divisible by an arbitrarily taken masking factor G and coprime to each admissible public RSA-exponent. The applicant further states(specification page 4, line 43-45) "The divisibility of the randomized blinding key by the masking factor G is achieved, in particular by correcting the output data of the random number generator with the help of the masking factor." The imposition of a correction factor to achieve divisibility, especially in the context of RSA, implies the use of integers when referring to multiples or divisibility.

In reference to claim 22:

U.S. Patent No. 4,759,064 by Chaum discloses a Blind Signature System comprising the steps of: "choosing secret factors (Chaum column 1, lines 22-24) and an RSA module corresponding to them(Chaum column 1, lines 27), choosing at least one admissible public RSA-exponent(Chaum column 1, lines 24-25), choosing initial data (Chaum column 1, lines 28), choosing a randomized blinding key(Chaum column 1, lines 44-45), choosing an encryption RSA-key whose module corresponds to the chosen RSA-module and with which key an RSA-encryption is performed while creating blinded data(Chaum column 1, lines 25-27, lines 44-47), the chosen initial data being processed with a result of the RSA-encryption while creating the blinded data (Chaum column 1, lines 43-47), arbitrarily choosing a secret RSA-key corresponding to the chosen secret factors and an arbitrary admissible public RSA-exponent (Chaum column 1, lines 26-30 and lines 43-45) and creating a digital RSA-signature on the blinded data corresponding to said secret RSA key(Chaum column 1, lines 44-47), creating an unblinding key corresponding to the blinding key and the secret RSA-key utilized while creating the digital RSA-signature on the blinded data which step of unblinding is performed by inputting said digital RSA-signature the unblinding key and the RSA-module into an unblinding converter whose output data are received as the digital RSA-signature on the chosen initial data. (Chaum column 1, lines 43-47)

Chaum, and the remaining art of record however fail to disclose the following:

- during the step of choosing at least one admissible public RSA-exponent a step of additionally choosing at least one basic public RSA-exponent is performed, for

each of which(basic public RSA-exponents), an arbitrary limiting multiplicity is chosen, and an arbitrary public RSA-exponent constituted from the chosen basic public RSA-exponents is accepted as the admissible public RSA-exponent,

- A multiplicity of each chosen basic public RSA-exponent being taken within a range of the chosen limiting multiplicity.
- During the step of creating the blinded data a step of RSA-encryption with the chosen blinding key is performed, the encryption RSA-key by which the step of RSA-encryption being performed during the step of creating the blinded data is chosen corresponding to an RSA-exponent constituted from the chosen basic public RSA-exponents each of which being taken in the chosen limiting multiplicity.
- The step of arbitrarily choosing the secret RSA-key corresponding to the chosen secret factors and arbitrary admissible public RSA-exponent is performed by arbitrarily choosing utilized multiplicities of the basic public RSA-exponents within a range of the limiting multiplicities of the basic public RSA exponents.
- The unblinding key is created by RSA-encryption in the system whereby each of the basic public RSA-exponents being taken in a multiplicity equal to the difference between the limiting multiplicity corresponding to said basic public RSA-exponent and the utilized multiplicity that was chosen in the step of choosing the secret key.

In reference to claim 28:

U.S. Patent No. 4,759,064 by Chaum discloses a system substantially similar to the apparatus disclosed in claim 28 which includes:

a blinding key choice unit having a random number generator (Chaum column 1, lines 44-45)
and a blinding unit having a modular exponentiator whose module input being connected to a module input of the blinding unit, and whose exponent input is connected to a blinding key input of the blinding unit, said blinding unit has an initial data input and one output being connected to a signature data input of a signature unit which has a secret key input and one output being connected to an unblinding data input of an unblinding unit which has a signature output, a module input, and exponent input and a blinding key input (Chaum Figure 1), characterized in that a base input of the modular exponentiator is connected to the initial data input of the blinding unit, and the output of the modular exponentiator is connected to the output of the blinding unit (Chaum Figure 1).

The prior art however, fails to disclose a system in which:

- The unblinding unit has additionally an initial data input and comprises a modular multiplicative Euclidean converter (MMEC) having a module input, base inputs and exponent inputs corresponding to each of said base inputs, the module input of the unblinding unit being connected to the module input of

the MMEC, the initial data input of the unblinding unit being connected to one of the base inputs of the MMEC, and an unblinding data input of the unblinding unit being connected to another base input of the MMEC, the blinding key input of the unblinding unit is connected to the exponent input of the MMEC which corresponds to the base input of the MMEC connected to the unblinding data input of the unblinding unit, and the exponent input of the unblinding unit is connected to the exponent input of the MMEC which corresponds to the base input of the MMEC connected to the initial data input of the unblinding unit, and the output of the unblinding unit is connected to the output of the MMEC, the blinding key choice unit comprises additionally an arithmetic controller with two limiting inputs which are accepted conditionally as first and second limiting inputs, the arithmetic controller being connected to the random-number generator, an output of the arithmetic controller is connected to the output of the blinding key choice unit, and the arithmetic controller is made so as to provide output data of the blinding key choice unit coprime to integers fed onto the first limiting input of the arithmetic controller, and to provide the divisibility of the output data of the blinding key choice unit with an integer fed onto the second limiting input of the arithmetic controller.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly be labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. This application is in condition for allowance except for the formal matters as noted above.

Prosecution on the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11, 453 O.G. 213.

A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

8/18/2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100